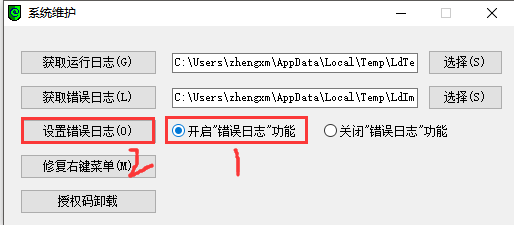
**本课题内容要点**

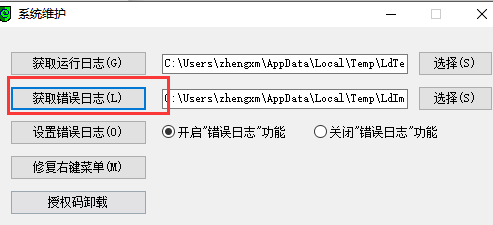
1. **Windows系统绿盾终端的错误日志简单分析。**
2. **Windows端绿盾服务端、终端的完整的运行日志获取位置（Linux和mac系统第一天有包含，这里不赘述）。**
3. **系统事件日志（以蓝屏日志的设置和获取为主）。**
4. **售后注意事项（反馈厂家技术问题时的几个要素、获取日志的及时性）。**
5. **第三方工具（procmon、fiddler、procexp）使用介绍（会提供文档）。**
6. **介绍已有的学习资料（每个功能的视频介绍）。**

**第一部分：Windows系统绿盾终端错误日志简单分析。**

1. 默认不启用错误日志，需要手动开启错误日志。日志名为：LdImportant.log如下图



1. 获取错误日志：如下图



1. 查看错误日志，一般应用于查看受控程序、密级、阅读权限等原因导致加密文件打不开。

例1：加密文件打不开，非受控程序去打开加密文件。

如果开启错误日志，获取错误日志，打开LdImportant.log会显示

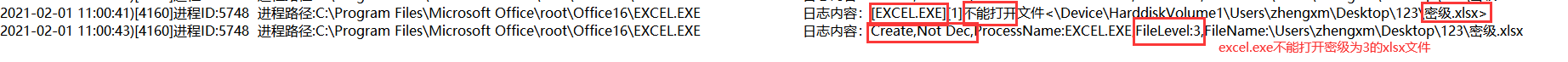


表示，excel.exe未受控打不开加密的测试.xlsx文件。这时，需要在绿盾控制台上针对该终端将excel.exe进程添加受控。

注意事项：不是错误日志有提示的所有进程都必须添加受控，比如一些安全软件，输入法等后台运行默认会去扫描打开加密文件，所以错误日志也会显示出来，但这些是不需要添加受控。

例2：加密文件打不开，低密级用户打开高密级文件。

如果开启错误日志，获取错误日志，打开LdImportant.log会显示2条日志：



（0公开文件；1内部资料文件；2秘密文件；3机密文件；4绝密文件）

例3：打不开不同一部门的加密文件



如上所示，该终端无法打开打开部门id为7，用户id为72的加密文件

**第二部分：Windows端，如何获取运行日志。**

当遇到技术问题，需要获取绿盾运行日志提供厂家排查时，该如何获取完整的运行日志呢。

**一、绿盾服务端运行日志获取：**

1. 引擎服务器日志获取位置：...Tipray\LeaderEIS\服务器\引擎服务程序\log
2. 采集服务器日志获取位置：...\Tipray\LeaderEIS\服务器\数据采集服务器\log
3. 绿盾控制台日志获取位置：...\Tipray\LeaderEIS\控制台\log
4. 服务器看护进程以及备份服务器日志获取位置：...\Tipray\LeaderEIS\服务器\log

**二、独立审批服务器日志获取：**

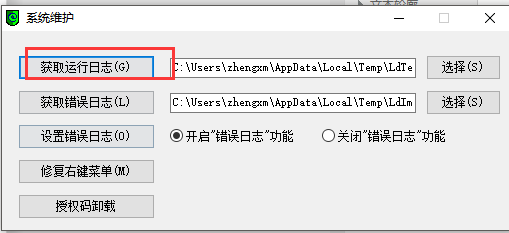
1、\TRWfe\TrwfeSync\log 2、..\TRWfe\logs\trwfe

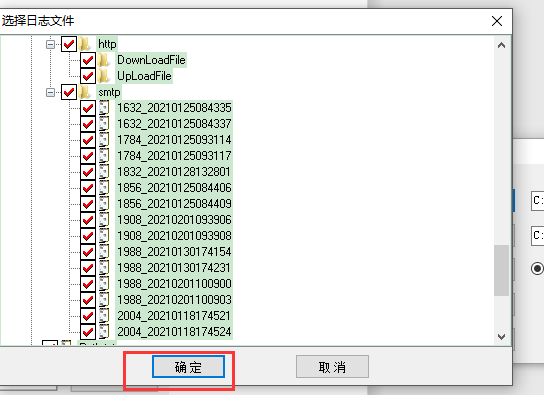
1. **移动服务端日志获取：**

1、...\TRMP\TRMPServer\log 2、...\TRMP\TRMPServer\logs

1. **绿盾终端运行日志获取：**

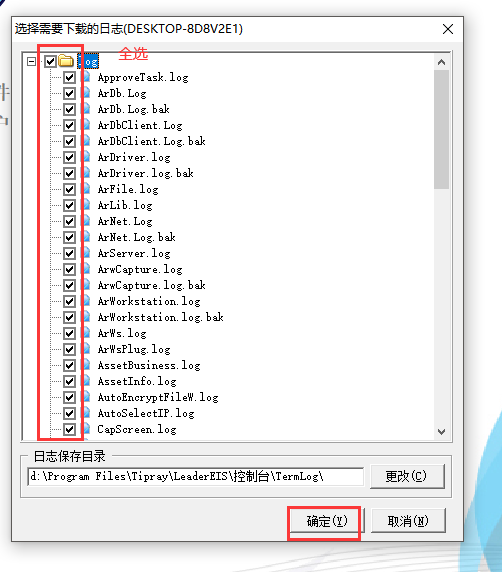
方法1：绿盾终端上获取，操作如下图:





方法2：通过绿盾控制台，远程获取





**第三部分：Windows端，系统事件日志查看。**

背景：遇到电脑蓝屏，死机，卡死等系统相关现象。需要查看系统事件日志或获取蓝屏日志分析的情况下。

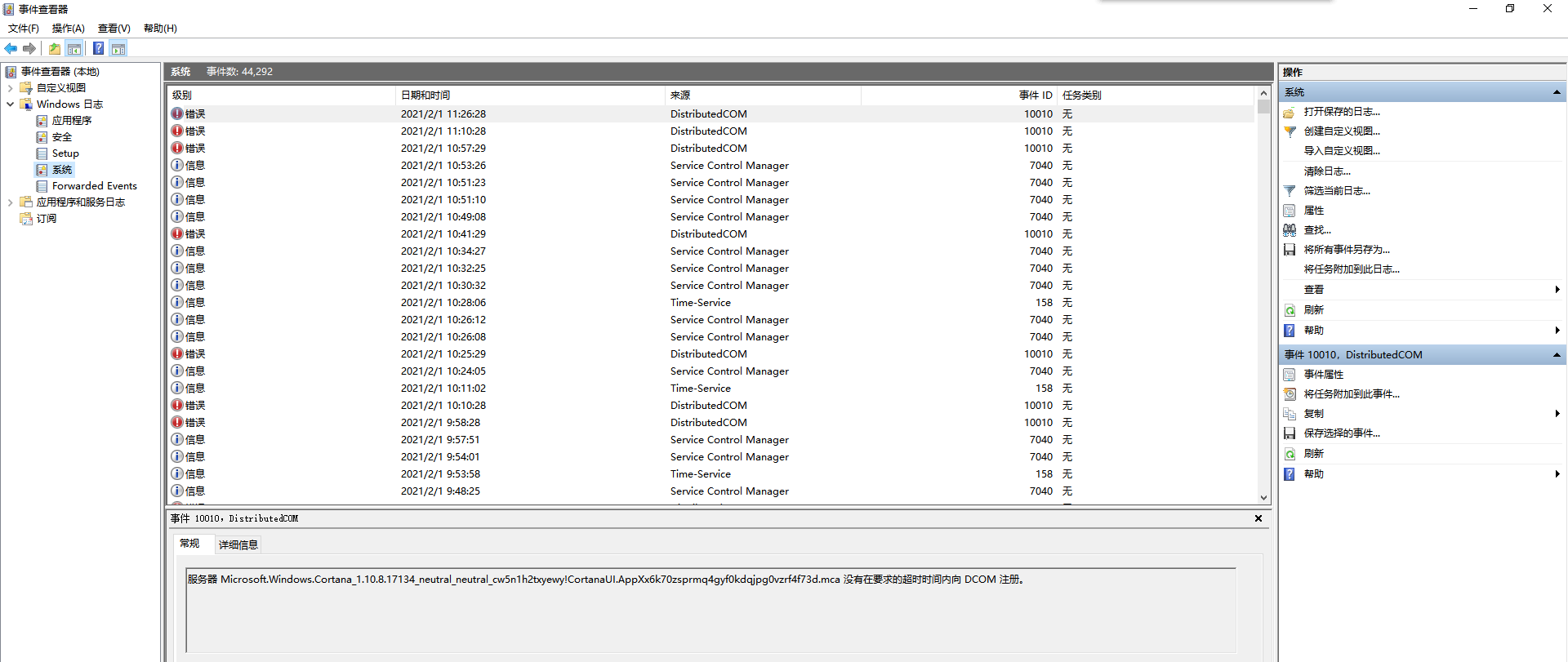
1. 系统事件日志方法：

打开事件查看器：

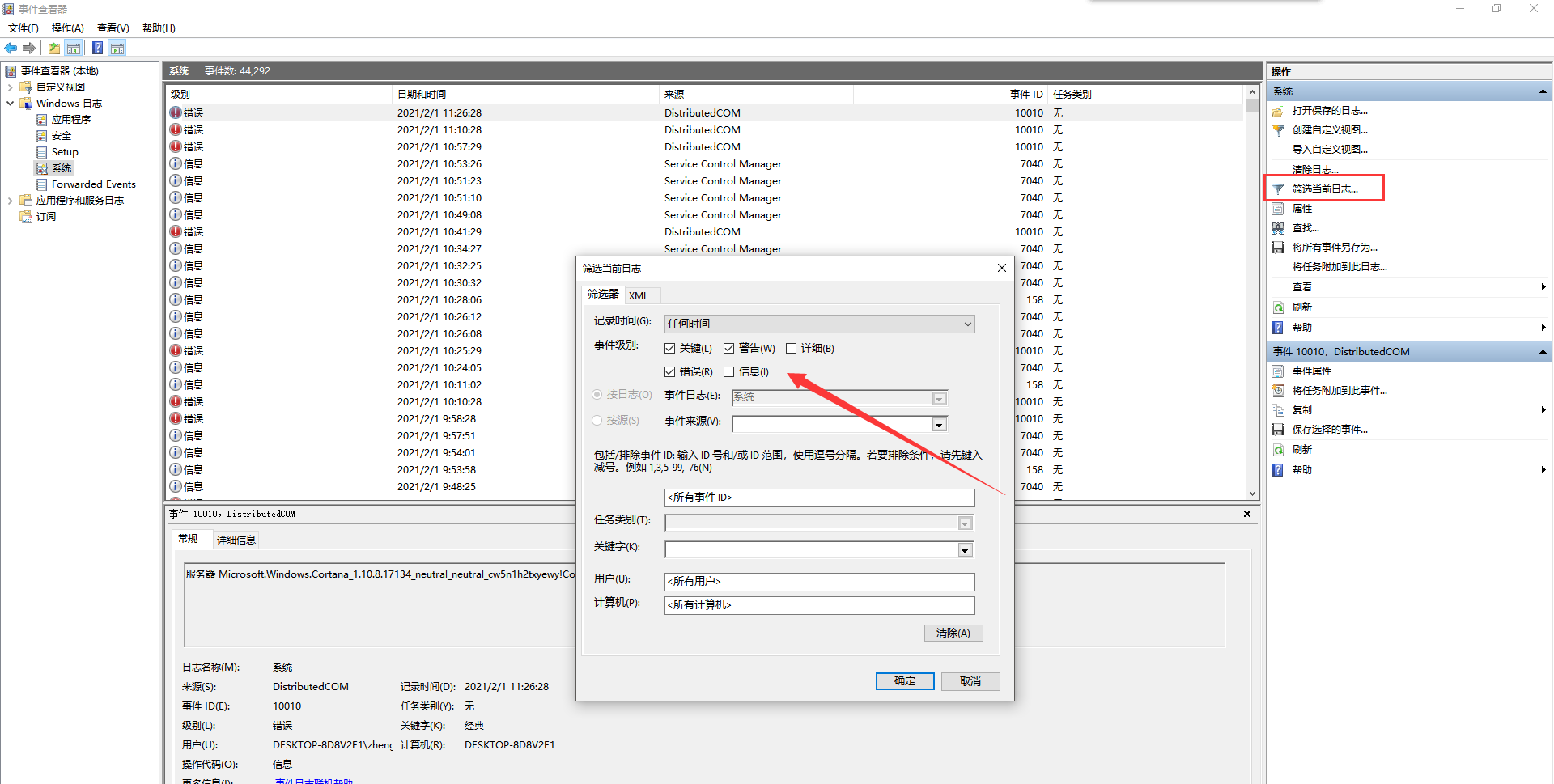
方法1：鼠标右击计算机→管理，找到事件查看器。

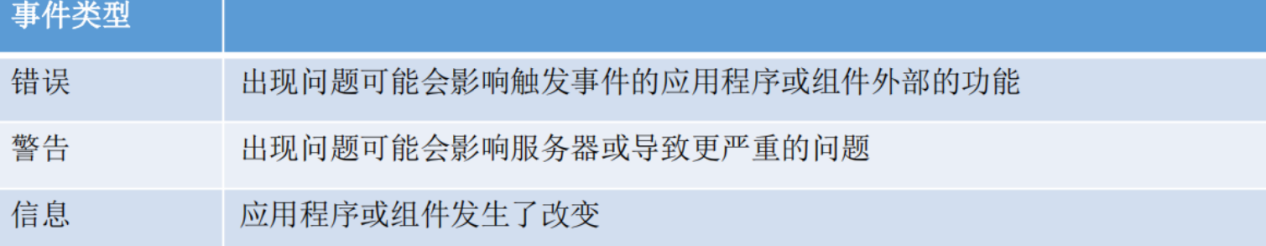
方法2：控制面板→管理工具 中找到事件查看器。

方法3：在【开始】→【运行】→输 入 eventvwr.msc 打开。



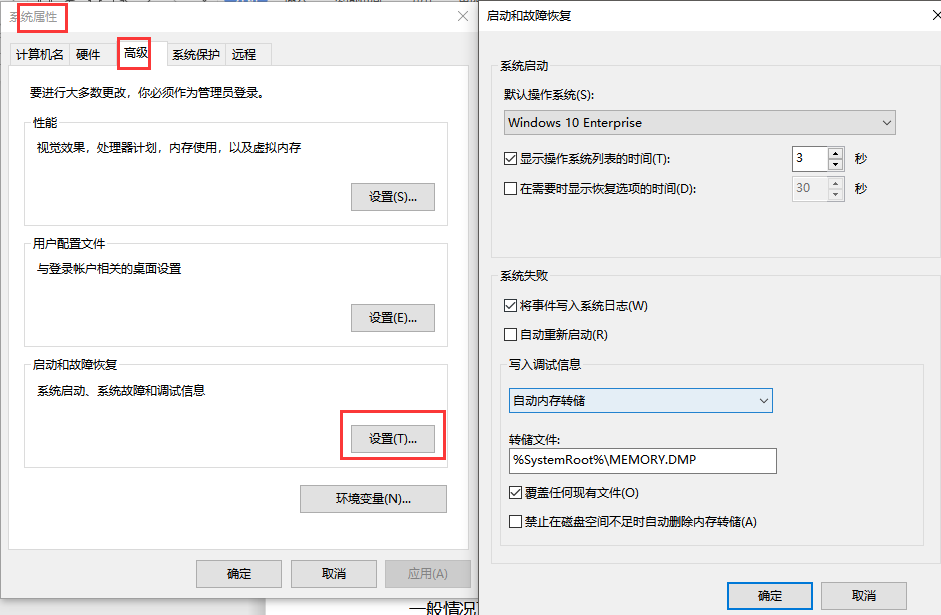
按需筛选日志：





1. 蓝屏日志设置和获取

鼠标右击计算机→属性→高级系统设置→(启动和故障恢复)设置→勾选“将事件写入日志系统”。



一般情况下，系统或自动写入，如果发生蓝屏后，看不到蓝屏日志，可以尝试将“写入调试信息”，调整小内存转储、核心内存转储或完全内存转储写入。

**小内存转储文件路径：C:\WINDOWS\Minidump\**

**核心内存转储路径：C:\WINDOWS\MEMORY.DMP  
完全内存转储路径：C:\WINDOWS\MEMORY.DMP**  
小内存转储，只是保存内存前64K的基本内存空间的数据   
核心内存转储，保存操作系统和相关系统级别服务的数据。   
完全内存转储，就是将内存中的数据全部保存，包括系统数据和用户数据。   
它们包含内存的范围从小到大，容量也是。

**第四部分：售后注意事项**

为了进一步提高处理效率，减少沟通成本，有利促进项目成功率，提出一些售后注意事项。

1. 客户名称
2. 产品版本（ex：绿盾版本:6.00 × v6.00.210201sc √）SC表示简体 TC繁体 SE英文

3、问题环境：物理机or虚拟机部署、操作系统（ex：win7旗舰版32位 or 64位）、是否能联网，是否有杀毒等

4、问题现象（ 问题现象发生过程，推荐带上现象截图）

5、自行排查到哪个阶段6、获取完整的运行日志或第三方工具日志（，及时性！）

相关联且重要的信息收集：1、文件名 2、时间点

注意事项：绿盾三代加密需要错误日志开启后一起获取

**第五部分：第三方工具（procmon、fiddler、procexp等）使用介绍（详见：文档）。**

**第六部分：介绍已有的学习资料（每个功能的视频介绍）。详见：绿盾产品功能视频(优酷) .xlsx**